# eSE technology update

***For GSMA TSG***

Gil Bernabeu
GlobalPlatform Technical Director

06/02/2020



GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

# Card specification evolution

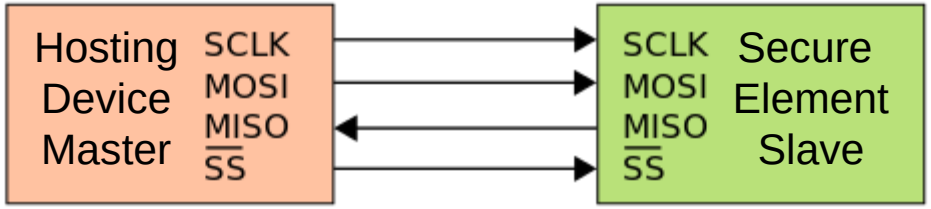
- The Card specification has been enhanced to answer multiple demands related to the massive integration of secure element within connected device and smartphone.
- This presentation highlights the main evolution and ongoing work

- The entire scope of the eSE has been enhanced
  - Physical Connectivity
  - Integration with device biometrics
  - One 2 many deployment or Application Store based deployment
  - Configuration and Functional compliance
  - Security compliance

# Physical connectivity evolution

## SPI – I2C support

- eSE are more and more connected using SPI or I2C protocols
- GlobalPlatform has standardized the transfer of APDU over these protocols in collaboration with ICA




The protocol manages also the power of the SE (wake up procedure) and 2 mechanisms for data retrieval

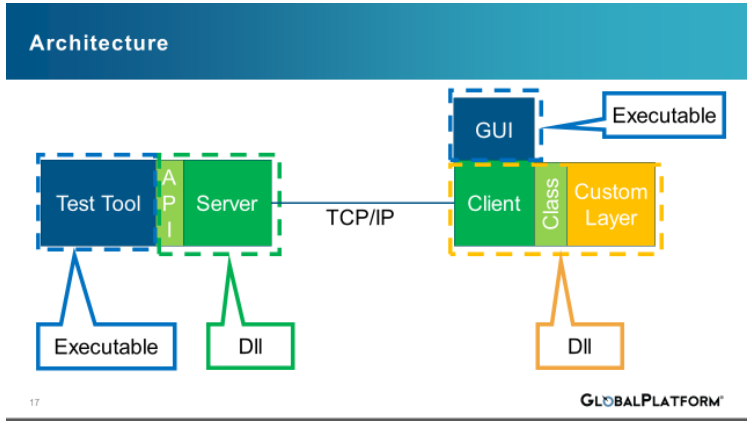
- Polling
- Interrupt

## SEs are now embedded in chipset as examples

- integrated SE
- SE stacked with NFC router

Testing and development are not possible using ISO readers

A new open source library is now available to manage communication with new form factor




https://github.com/GlobalPlatform/SE_Abstract_Communication_Layer_Over_TCP_IP

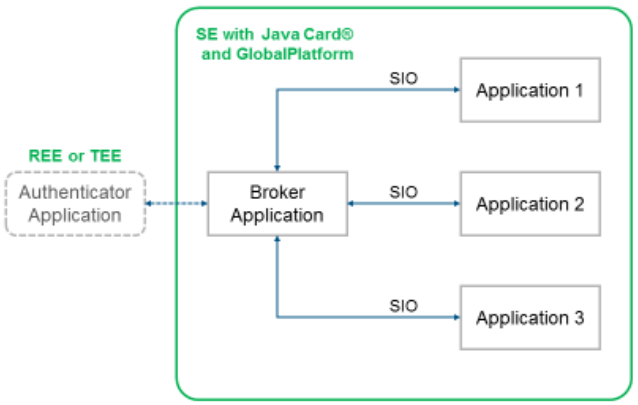


GLOBALPLATFORM®

# Broker Interface for Card Holder Authentication

- Multiple Applications hosted in the SE require Cardholder Verification.
  - EMVco has published requirements for CDCVM = Consumer Device Cardholder Verification Method
    - GlobalPlatform is also collaborating with FIDO Alliance on trusted User interface and biometrics
  - To simplify applet design, it is useful to centralize the management of Cardholder Verification methods and status and provide a standardized interface to such information

## Broker Interface API




- SIO: Sharable Interface Objects
- Broker Application registers as Global Service
- Push mode: All Applications are notified about a CV event
- Pull mode: Application queries for CV status

6

GLOBALPLATFORM

## CDCVM Types and Environments

**The following types are defined:**

Passcode / password
Fingerprint
Mobile device pattern
Facial biometric
Iris biometric
Voice biometric
Vein recognition (e.g. palm)

**The following environments are defined:**

Unknown or undefined entity
Using Rich Execution Environment (REE, i.e. Device OS)
Using Trusted Execution Environment (TEE)
Mobile Application (running in REE)
Digital Wallet (running in REE)
In the cloud
Application on this Secure Element
Application on another Secure Element

8

GLOBALPLATFORM



GLOBALPLATFORM®

# One2Many deployment

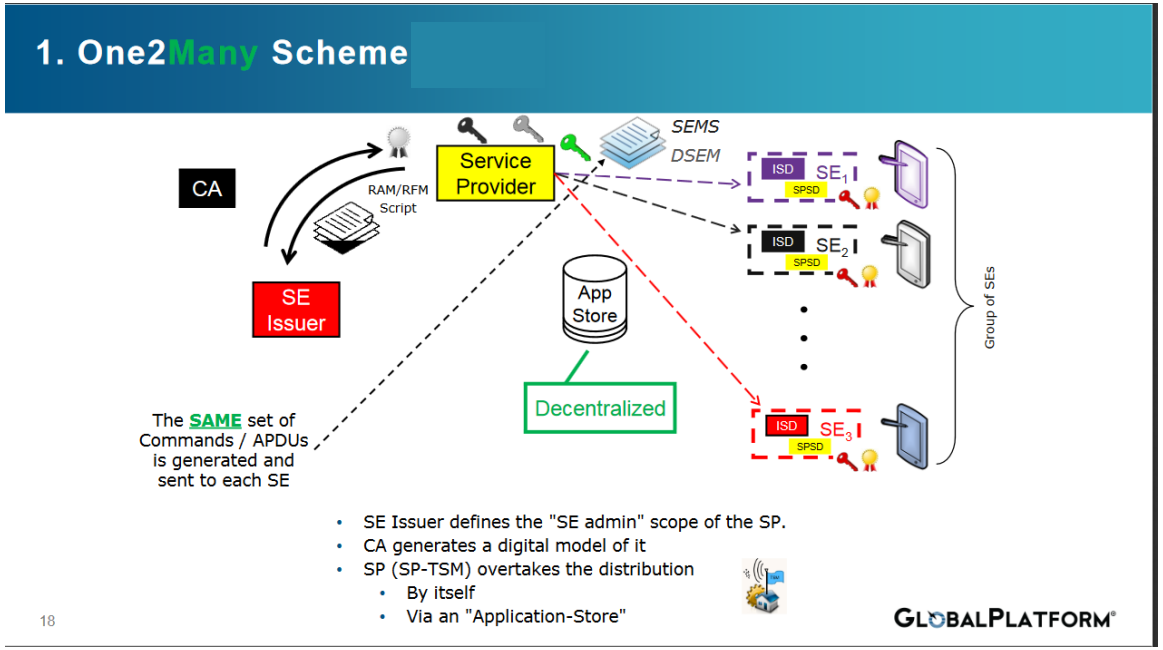
## Script-based

- Pre created script contains all commands to deploy an application (creation of SD, loading, installation)
- Rights are created via certificates of the Key used to protect the scripts
- One script can be applied to multiple SEs

## Decentralized and Asynchronous

- Scripts can be created in advance, store in an application package and executed later on into the device

- Two models available
  - SEMS and DSEM (SCP11c)






GLOBALPLATFORM

# SE configuration v2.0

- This document defines the minimum implementation requirements of the GlobalPlatform Card Specification for embedded Secure Elements.
- Such Secure Elements can be embedded in, for example:
  - a mobile device,
  - a wearable such as a smartwatch

- SE configuration
  - relies on GlobalPlatform Common Implementation Configuration,
  - references latest versions of GlobalPlatform Card Specification,
  - references latest
    - Amendment A – Confidential Card Content Management,
    - Amendment F- secure channels SCP11,
    - Amendment H -ELF upgrade mechanism-,
    - one-to-many management deployment models Amendment I -SEMS or Amendment F-SCP11c).

# SE PP

- The core SE PP defines the security problem, objectives, and requirements for SEs by extending the Java Card PP to address the security functionality defined in the GlobalPlatform Card Specification and Amendments.
- Six functional packages that address privileges.
  - Ciphered Load File Data Block, Global Services, Cardholder Verification Method (CVM), Delegated Management, DAP Verification, Mandated DAP Verification
- Four PP-Modules defined in the annexes of this document cover
  - Confidential Card Content Management ([Amd A]), Contactless Services ([Amd C]), Executable Load File Upgrade ([Amd H]), Secure Element Management Service ([Amd I]).
- A fifth PP-Module defined in the annexes addresses the post issuance OS Update capability.
- Conformance to EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5




GLOBALPLATFORM®